**REMARKS:**

This paper is herewith filed in response to the Examiner's Office Action mailed on October 31, 2007 for the above-captioned U.S. Patent Application. This office action is a rejection of claims 1-14 of the application.

More specifically, the Examiner has rejected claims 1-14 under 35 USC 103(a) as being unpatentable over Win (US6,453,353) in view of Wright (US20040123153). The Applicant respectfully traverses the rejections.

Claims 1, 9, 12, and14 have been amended for clarification. Claims 6-7, 10, and 13 have been amended accordingly. Claims 15 and 16 have been added. Claims 2 and 11 have been canceled. Support for the amendments can be found at least on page 7, lines 5-18, and page 8, line 29 to page 10, line 3. No new matter is added.

Regarding the rejection of claim 1 the Applicant notes that claim 1 has been amended to recite:

> A method, comprising: performing an automated security scan of a second network device by a first network device to determine a capability of the second network device; determining an attribute based, in part, on the determined capability; generating an attribute certificate based in part on the attribute; storing the attribute certificate including the attribute; and responsive to a verified authentication request, determining that the attribute certificate is valid and authorizing access to a resource over a network based, in part, on the attribute associated with the attribute certificate.

The Applicant notes that claim 1 has been amended to incorporate features similar to claim 2, and claim 2 has been canceled. The Applicant contends that claim 1 is clearly patentable over the references cited.

Firstly, in regards to both the rejection of claim 1 and the rejection of claim 2 the Examiner cites where Win discloses:

> "After a user is authenticated, the Authentication Client module 414 calls the Authorization service of Access Server 106. In response, the Authorization service requests profile information about the user from the Registry Server 108, as shown by state 520. In state 522, Registry Server 108 returns the profile information to Access Server 106. The profile information may comprise the user's name, locale information, IP address, and information defining roles held by the user. The Authorization service creates a "user cookie" 528 and "roles cookie" 530, which are used to convey profile information to browser 100. The "user cookie" contains a subset of the user profile information. The "roles cookie" contains a list of the user's roles," (emphasis added), (col. 10, lines 43 to 55).

As cited, Win merely appears to disclose that after a user is authenticated the Authentication Client 414 calls the Access Server 106 and in response the Authorization service of the Access Server requests profile information from the Registry Server 108. The Access Server receives the profile information and creates a "user cookie" 528 and a "roles cookie" 530 using the received profile information. Firstly, the Applicant notes that antecedent basis in claim 1 requires that the "verified user request" and "authorized access" are subsequent to performing an automated security scan of a second network device by a first network device is performed before the user is authenticated.

Further, Win discloses:

> "Using Administration Application 114, an administrator may find, list, create, delete and modify user, resource and role records. Each role record contains a name string, unique identifier, description string and additional fields or attributes. Each user record stores profile information. For example, the user record profile information includes the user's first and last names, email address, login name, password, locale, whether the account is active or inactive, and when the password or account will expire," (emphasis added), (col. 13, lines 8-16).

The Applicant submits that the profile information is entered by the Administrator using the Administrator Application 114. Further, the Applicant notes that the profile information relied on to create the "user cookie" as cited in Win is the same information entered by the administrator

using the Administration Application 114. The Applicant contends that this profile information used by the Authorization service of the Access Server 106 to create a "user cookie" can not be seen to come from a device performing an automated security scan of a second network device by a first network device to determine a capability of the second network device as in claim 1. The Applicant contends that Win clearly does not disclose or suggest at least where claim 1 recites "performing an automated security scan of a second network device by a first network device to determine a capability of the second network device; determining an attribute based, in part, on the determined capability."

In regards to Wright the Applicant notes that Wright relates to a method to provide diagnostics for a mobile device as well as a method to restrict access to data by a mobile client based upon the location of the mobile device, the security policy applied in the mobile device, and/or the security features of the mobile device, (Abstract, paragraphs [0046]-[0047]). Wright discloses that software modules installed on the mobile device monitor the security settings and related information on the mobile devices, (par. [0066]). In addition, in Wright the software modules on the servers and the mobile devices allow secure communication of the diagnostics information and security policy settings between the mobile devices and the servers (paragraphs [0057]-[0059]).

In the Office Action the Examiner states:

> "Win does not explicitly teach determining an attribute based, in part, on a capability of the network device. Wright teaches the feature of determining an attribute based, in part, on a capability of the network device ([0066-0067], [0078]-[0121])"

As cited Wright discloses:

> "The illustrated system 201 embodiment in accordance with the present invention further comprises a security feature module 210 for determining whether one or more security features have an activity status of inactive or active in a communication session between the mobile device and another computer. An example of a security feature is a connection type of wired or wireless. [...] Furthermore, different security policies may be assigned based on the operating

> system employed or the version of the operating system because different systems or versions provide different security features. Furthermore, different policies may be employed based on the security features (e.g. a firewall) provided by different types of network access points (NAP)," (emphasis added), (par. [0066]).

The Applicant notes that Wright as cited discloses that the security feature module 210 is determining whether security features are active or inactive. However, the Applicant submits that here the determining of security features **of the mobile device** is performed by the security feature module 210 embodied **on the mobile device** itself (par. [0058] and Fig. 2B). Thus, here Wright can not be seen to relate to performing an automated security scan of a second network device by a first network device to determine a capability of the second network device as in claim 1.

Further, as cited Wright discloses:

> "In the system embodiment of FIG. 2A, the policy management module 236 defines 302 a security policy applicable to a client mobile device based upon criteria. One example of criteria is the location associated with the network environment in which the mobile device is operating. Other examples of criteria are the presence or the activity status of one or more security features. Of course, a combination of location and one or more security features may also form a criteria basis for defining a security policy," (par. [0078]); and
>
> "One aspect of client management is that the policy management module 236 maintains 314 client management information for the mobile device and the one or more policies associated with it. The following list of information fields is an example of the types of information which may be included in client management information," (par. [0104]).

The Applicant submits that the criteria and the client management information for the mobile device in Wright is not seen to be determined by performing an automated security scan of a second network device by a first network device to determine a capability of the second network device as in claim 1.

Wright discloses:

> "The server or server-side system 200 allows an administrator to manage and distribute policies and software upgrades, analyze logs, and perform remote diagnostics. [...] The client side system 201 monitors the user's changes in location and/or security features and applies the appropriate policies automatically as the user moves about or different security features are activated or deactivated. The client 201 enforces the policies set up by the administrator, and performs diagnostics.," (par. [0046]); and
>
> "The policy distribution module 234 has a communication interface or is communicatively coupled to the policy management module 236 for receiving notifications of updated security information. Examples of security information are versions of existing policies, policies, or software," (par. [0051]); and
>
> "The location detection module 208 detects or determines the location associated with the current network environment based upon criteria defined in a downloaded policy from the server system 200. In this example, the policy setting module 212 receives, installs and updates the security information including security policies and/or software updates received from the policy management module 236 via the policy distribution module 234 over the network connection 204.," (par. [0061]).

The Applicant notes that Wright discloses that the policy management module 236 is in communication with the modules of mobile device to receive notifications and distribute security policies, (see Figs. 2A and 2B). The Applicant contends that Wright does not disclose or suggest at least where claim 1 recites "performing an automated security scan of a second network device by a first network device to determine a capability of the second network device."

For at least the reasons stated the Applicant contends that the references cited can not be seen to disclose or suggest claim 1 and the rejection of claim 1 should be removed.

In addition, as the independent claims 9, 14, and 16 recite a similar feature of claim 1 as stated above, the references cited are not seen to disclose or suggest all claims 1, 9, 14, and 16. Therefore, the rejections of these claims should be removed.

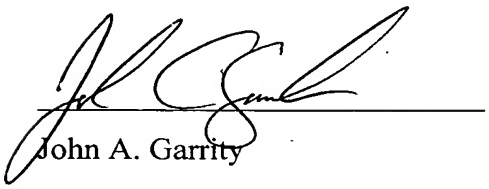
Furthermore, for at least the reason that the claims 3-8; and 10 and 12-13; and 15; depend from

claims 1, 9, and 14 respectively, the references cited are not seen to disclose or suggest these claims, and the rejections of all claims 1, 3-10, and 12-16 should be removed.

Based on the above explanations and arguments, it is clear that the references cited cannot be seen to disclose or suggest claims 1, 3-10, and 12-16. The Examiner is respectfully requested to reconsider and remove the rejections of claims 1, 3-10, and 12-16 and to allow all of the pending claims 1, 3-10, and 13-16 as presented for examination.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record. Should any unresolved issue remain, the Examiner is invited to call Applicants' agent at the telephone number indicated below.

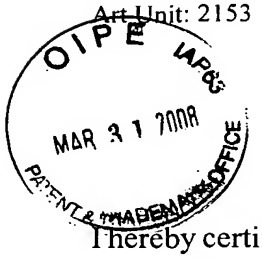
Respectfully submitted:



Mar 28, 2008

John A. Garrity
Reg. No.: 60,470
Customer No.: 29683
HARRINGTON & SMITH, PC
4 Research Drive
Shelton, CT 06484-6212
Telephone: (203)925-9400
Facsimile: (203)944-0245
email: jgarrity@hspatent.com

Date




## CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

March 28, 2008
Date

Deborah Forsyth
Name of Person Making Deposit